PART III. NETWORK MANAGER'S GUIDE

CHAPTER 6
NETWORK MANAGER'S GUIDE

6.1 Introduction

This section of this guide identifies some of the major steps to be taken when planning, implementing, and operating a network, specifically an HF ALE radio network. This guide identifies some of the pitfalls that could occur when implementing a network, and it presents a series of rational and orderly activities to support the planning and design process. Adherence to these guidelines could significantly minimize implementation risks.

The following is also a guide for understanding duties and functions associated with the position of *Network Manager* for a typical HF ALE network. The network manager and the network engineer work closely together to design and implement a smoothly functioning, efficient network. The term network manager refers to the function of network management, possibly a team of people, rather than a single individual holding that title. The network manager team has historically been responsible for the selection, implementation, testing, expansion, operation, and maintenance of the communication network. There are two primary objectives of network management: 1) to satisfy system users, 2) and to provide cost-effective solutions to the organization's communication requirements.

A summary of the duties of the network manager include the following:

- Work closely with the network system engineer to implement the details of the network design and to tune the specific network for the job at hand;
- Work closely with the network engineer to establish the physical network layout;
- Establish the necessary ALE network parameters and procedures;
- Be responsible for the establishment and maintenance of frequency sets and frequency assignments for the network;
- Be responsible for the establishment and maintenance of station addresses and associated parameters;
- Be involved in establishment of network operational procedures and disciplines needed for a smoothly operating network;
- Train and assist users in setting up or programming their equipment to assure smooth compliance with network operations procedures, and
- Be responsible for resolving network operational problems such as interference congestion, or faulty operator training.

The network manager is a key figure in all phases of network planning, implementation, and operation. A summary of these phases might be as follows:

- Planning,
- Implementation,
- Site Preparation
- Installation
- Pre-Cutover
- Cutover
- Operations [Wetterau, 1991].

6.2 Managing the network role of the network manager in an HF ALE radio system

The network manager has primary responsibility for the day-to-day operation of the particular HF ALE Radio communication network. His/her duties prescribe that he/she must be aware of all the underlying details of the network's operation as well as the personnel who staff the various stations within the net. The network manager must have a good understanding of the unique skywave propagation characteristics of HF radio as well as those of ground wave and line-of-sight propagation. He/she must be familiar with the various details and characteristics of HF ALE Radio equipment so he/she can guide the procurement, the setup, and the day-to-day functioning of the network operation.

The first preliminary phase of designing a new communication network is the *planning segment.* The major steps in network planning segment might include:

1. establishing objectives and requirements of the network,
2. doing a benefits and cost analysis,
3. doing network design to include network layout and site selection, and
4. doing equipment selection and procurement.

6.2.1 Network planning

Objectives and requirements

Objectives and requirements definition can be a very important prerequisite before any decisions on design alternatives can be made. This definition phase can be an iterative process where one examines the known requirements and then formulates a series of conceptual network solutions. The network manager should initially be provided with a list of network requirements and objectives, if not he or she should gather these facts from prospective users of the network. Usually it is well recognized that a need for the network exists, but different users may have different views of what the objectives and requirements of the network might be. In seeking out requirements, the network manager must be careful to determine why a requirement exists and if that requirement is real or imagined. It will be the job of the network manager to pull together the requirements and objectives,

sift though them to find common threads, and to see if he can get the users to agree on a network architecture.

The requirements of a network can be described as falling into three general categories: Service Requirements, Interconnection Requirements, and Network Level Requirements.

The *Service requirements* include items such as:

1. overall scope of the network,
2. the nature of the network services to be included,
3. types of traffic to be carried,
4. costs involved, and
5. possible schedule constraints.

The *Interconnection Requirements* include those communication characteristics that relate to the paths within the network. Examples of these characteristics might include the location of nodes and resources; traffic classes between nodes; average traffic volumes; peaks and valleys of traffic volume; aggregate traffic flow; network performance; network security issues; and network availability issues.

The *Network Level Requirements* include issues beyond the functional characteristics (i.e., traffic, performance, security, and availability) such as network maintenance, network growth, and network management and control.

Benefits and cost analysis

The requirements analysis justifies the network architecture and quantifies user needs that will be met by the new network. The network designers uncover the technical needs and establish the network's benefits. Some of the issues that justify the network might be: the additional communication that it enables, the savings accrued from task reduction when it is deployed, the efficiency of traffic that can be handled, or the more traffic throughput that can be expected. Thus a benefits and cost analysis can show what are the true costs (in terms of money and perhaps in terms of performance) of networking for all the users.

Network design

Using the objectives and requirements as a basis, the analysts can perform a *network design.* The network manger must work with the network engineer to do the network design to include network topology, network layout, and site selection. The network topology may be chosen based on where the traffic originates , the destination to which it is to be transmitted, and the projected data flow. The topology chosen could be point-to-point, star, mesh, multiplexed, *etc.* The topology might consist of a single network or a multi-network environment (*i.e.,* a collection of networks linked together for communication). A traffic analysis can be used to show where traffic may be high or low, sporadic, priority or non-priority.

The network manager will identify all the stations or nodes to be included in the network as well as their geographical locations. He must be aware of the physical location of each node and the relationship to other nodes in the network. He must acquaint himself with any physical obstacle (*i.e*., mountains, buildings, antenna, *etc*.) which may be present in the paths between the various nodes. He should be acquainted with the equipment located at each node especially the power and antenna characteristics. He must be keenly aware of all the various propagation paths between the various stations involved (*i.e.*, skywave, ground wave, and line-of-sight). The network manager will need to know details about the characteristics and volume of the communications traffic that will be traveling between the various nodes at various times during the day. He must be aware of the communication interfaces that are connected to each node and how the loss of one or more of these interfaces could affect message traffic across the network. The manager must be made aware of the priority of messages through each node as well as the importance of each net member to the total mission of the network. If messages are to be forwarded through intermediate nodes to accommodate the case where coverage may not be universal, this special routing must be considered in his traffic analysis.

To identify answers to the many questions the network manager may have at this point, he may wish to send a questionnaire to the managers of each potential node in the network. The purpose of the questionnaire will be to identify resources and equipment; availability of personnel; equipment types; traffic volumes; traffic classes; peak/normal loads; protocol overhead; performance considerations; reliability and availability considerations; aggregate traffic flow determination; and any special security, maintenance, management, or growth issues that might surface from this particular node.

1. Physical location. One of the first elements of the functional interconnection requirements is determining the *physical location* of each user or node of the network. The questionnaire should attempt to make a determination regarding the site location, general terrain considerations, *etc*. The identification process will also include the determination of whether the physical facilities are already occupied, are under construction, or are only be in the planning stages. The site may be a staffed or a remote unstaffed site.

2. Equipment type. It will be essential to identify the types of *existing equipment* located at each node including models, vendor, revision, memory/buffer capacities, power, antenna, etc., so its performance in the network can be modeled. Different equipment will have different address buffer sizes, link quality assessment (LQA) storage and reporting capabilities , traffic pattern paths, connectivity matrix capabilities, and message buffering capacities. Also the radio units will be of different networking capabilities (*i.e.* null datalink controller, basic network controller, hub network controller, *etc*.)

3. Traffic. The questionnaire should determine *anticipated traffic requirements* of each node. The traffic requirements encompass one of the most important characteristics to be accounted for in

the network system design. Knowing the peak, null, and aggregate traffic volumes of each node will allow the network manager to determine these values for the entire network.

4. Traffic classes. One way to begin defining traffic requirements is to determine the general *traffic classes* used by each node. These classes might include the need for real-time or immediate responses as well as the possible need for priority message traffic. The traffic may be interactive requiring ACK/NAK responses or may be simple broadcast mode. The traffic may be simple AMD messages or may be large blocks of data to be transferred between host computers or peer devices. The network manager is best advised to view file transfers of large blocks of data as only allowable under special conditions. The transfer of large blocks of data can be very time consuming and can tie up the network for long periods. For instance, if large block transfers were allowed, the normal traffic load could be delayed for minutes at a time; in general, this sort of traffic tie-up is an unacceptable practice. Data transfers of large blocks of data should be accomplished by other means (*i.e.*, data modem, *etc.*), rather than as traffic on the network.

   Another factor affecting traffic volume and the network as a whole is the protocol In general the overhead for most HF ALE radios will be approximately the same, but it could vary by equipment vendor, by the operator□s chosen variables, by the type of commands being used (*i.e.*, procedural or control), by whether the message traffic contains LQA and AMD orderwires, and by use of data transfer protocols (such as DBM, DTM, *etc.*).

5. Performance A node may have special requirements in terms of *performance.* Performance may be defined for the network, for an individual path, or for an individual node. An individual node, in turn, may need to define acceptable delays according to mission, scenario, or logical path.

6. Availability/Reliability. The questionnaire should be structured to determine the *availability and reliability* requirements of the node. A node might have a need to define the minimum requirements for availability or reliability. The network manager might need to know about the user's sensitivity to transfer or duration failures. He will also have to make a determination of what is the tolerable impact of a failure on the user's operation. He might also have to study the results of losing a particular node to overall network operation such as when the network is no longer being able to use this node for forwarding messages. When designing a network for circuits with high priority traffic or network links that must have a high degree of availability, the network manager may conclude that the links should use redundant equipment for backup purposes. It might be necessary to have a complete backup of critical equipment installed and available in a powered-up "hotstack" to be used in case of failure. For the most critical paths and to increase the redundant capabilities of backup equipment, this equipment could be connected in a "mirror" configuration where the frequency scan list and address information matrixes of the backup equipment is as current as possible. This current information is achieved by constantly updating both the on-line and backup databases.

7. *Security.* The questionnaire should be designed to identify and evaluate any special *security* issues associated with this particular node. Security requirements can also be applied to individual nodes and to the network as a whole. Like reliability, there is a real cost associated with security; for that reason, it may be wise to determine precisely which paths and messages must be secure. The network manager should also make an attempt to address security in terms of physical facilities, access to the network, and the data itself.

8. *Maintenance.* The questionnaire should be designed to determine if any special *maintenance* requirements will be needed. Maintenance requirements will be dictated to a large extent by the availability requirements of the network. Preventive maintenance procedures should be implemented to maintain the hardware and software of the system. These maintenance procedures should be put on a scheduled program to assure that the procedures are undertaken at the prescribed interval.

9. *Network Management and control.* The questionnaire should be structured to determine what degree of network management and control will be needed. *Network Management and Control* requirements include such items as the design of central communication points and the handling of various types of information needed for control purposes.

10. *Growth*. The questionnaire should be designed to determine the anticipated growth issues of the node and network as seen by the individual node administrator. The issues of size and *growth* of the network should be resolved by accommodating decisions made in the requirements phase. Growth may be the result of adding new nodes, developing new applications, changing security requirements, and/or changing performance levels. Users often are more concerned with day-to-day operations than with long-term growth issues, and therefore it will be the network manager's responsibility to ask penetrating questions regarding long-term growth requirements.

Functional Design

Having analyzed the requirements and received responses from the node managers on the details for each node, the network manager has an insightful perspective of WHAT the network is to do. The task now is to translate the requirements into a functional design. The objective is to develop a network design that satisfies as many of the requirements as possible.

One of the first requirements that must be translated into design criteria is the user's expectation of *network performance*. Users perceive the network's performance in terms of *delay* experienced in getting a message to another user. This delay is usually measured from the first character of the request to the last character of the response, or the total time the channel is tied up with passing this message. Another type of delay is associated with an intermediate node in message forwarding. The delay here might be due to queuing the message for later transfer. This delay can be more significant than normal message passing but possibly not as great as the delay experienced with a switching node. A switching node is acting as a bridge between networks and possible buffering, decompression, queuing, compression, unbuffering can be taking place. By far the most significant

contributor for delay in a HF ALE radio system is due to the changing HF Ionosphere conditions associated with the atmosphere. In some cases the delay experience by a particular message might be 12 to 24 hours or longer. HF ALE radio usually has several frequencies associated with a system in which case the delay may be associated with changing to another frequency. Or in the case of a complete shut down of all frequencies used by this station, delay would be until conditions change

The next issue to be addressed by the designer is that of network *throughput.* Throughput is typically defined as the rate at which data transfer can be sustained. To a very large extent, this is limited by the speed of transmission, delays due to distance, delays through nodes, possible switching delays, *etc*.

The *availability of a network* is usually expressed as the percentage of "up-time." It is determined by dividing the Mean-Time-Between Failure (MTBF) by the sum of the MTBF and the Mean-Time-To-Repair (MTTR). The availability is calculated for each component in the network, and the product of the availability of the components in a given path yields the overall availability of the path [Rothberg, 1988].

Design Methodology

Given the requirements and analysis of the design criteria, one can look at the *Topological Design* of the network. Typically, the network design can be divided into two areas: 1) the backbone design where the backbone topology is characterized, and 2) the local access design where local node characteristics are added issues [Rothberg, 1988].

At this point the *connectivity* of each node can be determined. By determining primary and alternate paths across the network, connectivity to all nodes in the network can be determined as well as connectivity plans covering all nodes in outage conditions (such as bad propagation or failures of primary nodes). A simple graph is a useful tool in analyzing the connectivity of the network.

Now applying the connectivity and the *delay analysis* done earlier, the delay for each path can be determined. In some cases multiple hops or store-and-forward message delivery may be required to connect all nodes under all conditions.

If store-and-forward capabilities will be necessary to cover cases where a blockage has occurred, some basic queuing analysis will have to be applied to account for the time that messages are sitting in queues waiting to proceed to the next node. The most common queue is a single-server queue where messages or packets arriving randomly are serviced one at a time before being forwarded to the next node. A single-server queue might best be compared with a *line at a bank teller* [Rothberg, 1988]. Another type of server is a multiserver that handles arriving messages (packets) that have formed a single queue or line. A good example of this type of queue is a *single line at a bank or airline counter, where the next available teller or agent takes the next person in line* [Rothberg, 1988].

Variables associated with queue theory might be:

1. The number of messages arriving within a defined period,
2. The time required for processing each transaction,
3. The percentage of time a user should be able to access the network without being blocked,
4. Number of required servers,
5. The time required before a message is dropped due to continued blockage.

Simple queuing models are available for this analysis, should they be necessary.

Equipment selection and procurement

Part of the manager's duties in the planning function may include equipment procurement. It may be that the users themselves will procure their own equipment for individual stations, but there usually is some common equipment such as a master node, antenna, *etc*., that must be purchased by the network manager. Also the users themselves may need some expertise in the procurement process and may call upon the network manager for assistance. The network manager should be a key figure in the *equipment procurement process*. The network engineer and the network manager usually have the most current and relevant information about the network, its equipment, and its mission. The procurement officer will need to draw on this knowledge when purchasing equipment for the network or for the individual nodes. It should be the network manager's responsibility to be available for consultation on matters related to equipment purchases.

Designing for efficiency

After the first cut at a network design is finalized, the network management team should step back and take very special note of any evident inefficiencies. The inefficiencies of such a design may be overcome by combining some paths, hardware, communications facilities, or other resources into a single integrated structure.

6.2.2 Network Implementation

The second phase of network planning is the *implementation phase*. Implementation can include the items of planning, schedules, and control. Since the network manager is responsible for the network in its entirety, he is the logical candidate for responsibility when it comes to initial planning and setting the schedule for the events that must happen for the network to become a reality. The network manager must also set up operating procedures that will assure that the network operates as everyone expects. The procedures will include perhaps unique characteristics or parameters, frequency sets and assignments, and individual and network addresses, and network standard operating conditions.

Network development requires an orderly and structured approach, as would be expected in any design activity. The phases of the network development life cycle might include:

1. Requirements definition,
2. Feasibility determinations,

3. Design constraint analysis,
4. Network loading analysis,
5. and Network Design.[Rothberg, 1988]

The network manager develops a *system implementation plan* with the primary purpose to identify all the necessary resources, activities and phases of the development life cycle.
The topics to be included in the implementation plan might include:

1. Functional overview and scope statement - outlining the network in terms of the services it will offer,
2. Estimate of overall project costs,
3. Estimate of project completion date which possibly might be supported by:
    a. detailed activity schedules,
    b. and/or milestone charts
    c. cost-resource requirements for each activity,
    d. project organization to identify personnel requirements—technical and supportive
    e. Assumptions that may have been used to arrive at the technical, cost, or schedule aspects of the program.[Rothberg, 1988]

Unique ALE parameters

The network manager must work with the network engineer to do the network design to identify any unique network (ALE) parameters. These items might include important details and trade-offs that are associated with setting-up and maintaining a HF ALE Radio network. Power, antennas, frequencies, address name groupings, etc., all can effect the operation of the network. The network manager, together with the network engineer must develop these details for the benefit of all network users and the efficiency of the total network.

Frequency sets and frequency assignments

The network manager must establish and maintain the frequency sets and frequency assignments necessary for network operation. The radios are capable of scanning a group of select frequencies or channels under manual control or under the direction of an automatic controller. The scanned channels should be selective by groups or sets, and also individually within the groups, to enable flexibility in channel management and network scan management.

The selection of optimum operating frequencies is one of the most important characteristics contributing to overall system performance. The frequency (cies) should be chosen based on the following general characteristics:

1. The frequency (cies) chosen is (are) has to be one of the assigned frequencies given to the net;
2. The propagation of that frequency is in the selected range which ensures signal-to-noise-ratio (SNR) or maximum signal reaching the receiver and minimum distortion;

3. The frequency(cies) chosen must propagate(s) well during at least some periods of the day (considering the whole 11-year solar cycle);
4. Be environmentally noise-free of man-made noise at least during some hours of the day; and
5. The propagation path between both end points should have similar characteristics in both directions during some period of the day

The network manager typically has a group of frequencies assigned to the network. He may or may not make them all accessible to all the members of the network. He may wish to distribute the frequencies across the network in a manner that establishes *subnetworks*. As an example, suppose the network is assigned 10 frequencies, but at the network manager's discretion, node 1 can only use channels 0,1,2,8,9, while node 2 can use channels 2,3,4,5,6,7,8. It is clear that for traffic between node 1 and 2, only channels 2 and 8 are in common and therefore one of these channels must be used for communication between these nodes. Each of these groups of frequencies is considered a *set* and the typical network can have as many sets as needed. The determination for sets might be physical location, stations with characteristics in common (i.e., mission, type, propagation limitation, etc.).

Refer to FED-STD-1045 for additional information on frequency sets and frequency assignments.

Station and network addresses

HF ALE stations are assigned one (or more) addresses to identify them during selective calling. The two basic types of station addresses are: *individual addresses* and *net addresses.*

The network manager must establish and maintain the individual and net addresses of the network. For some DoD and Federal networks, ALE addresses must be assigned and registered[1].

1 Proposed FTR1047/3 Network Coordination and Management- ALE Addressing and Registration, establishes procedures for the assignment and registration of ALE addresses for use in network operations in the DoD and Federal communities. This standard also provides guidance for closed departmental network operations and directives for intra-department and shared network operations [proposed FTR 1047/3]

An individual address is unique and is assigned to only one station in the network. Calls to individual addresses are responded to by only one station. Net addresses can be assigned to a group of stations that might have something in common within the network (*i.e*., mission, type, propagation limitation, *etc*.). Calls to net addresses are responded to by more than one station but require individual stations to respond only in predetermined time slots associated with that station individual address. There may be many nets associated with a network. Each station may have more than one individual, or net addresses. Wildcard addressing (Anycall or Allcall) can be used to further modify station addressing by changing the grouping of sets responding from "one," to "many," or "all." [2]

Individual Self-Addresses: All ALE stations have the capacity to store and use at least 20 individual self-addresses, each having 3 to 15 characters. If the address is only 3 characters in length it is termed a *basic address;* if from 3 characters to 15 characters, it is termed an *extended address.*

Multiple stations: A prearranged collection of stations, with a commonly assigned address is termed a *net*. A non-prearranged collection of stations without a commonly assigned additional address is termed a *group*.

Net: A prearranged collection of stations.

Group: A non-prearranged selection of stations. In many cases, little or nothing is known about the stations, except their individual addresses and scanned common frequencies.

Network Self-Addresses: A net address is an address used to place a call to a prearranged group of stations that share a common address. A net call rapidly and efficiently establishes contact with a prearranged group of net stations by using a single net address, which is an additional address assigned in common to all net members.

Utility symbols in address: Addresses may be modified in some cases through the use of the utility symbols "@" and "?". These special utility symbol characters are used in the special calls such as:
- Stuffing
- Allcalls
- Anycalls
- Wildcards (after FED-STD-1046 /1)
- Self address
- Null Address

Stuffing. The quantity of available addresses with the system, and the flexibility of assigning addresses, are significantly increased by the use of address character stuffing. This technique allows address lengths, which are not multiples of three, to be compatibly contained in the standard (multiple of three) address fields by stuffing the empty trailing position with the utility symbol "@". Refer to FED-STD-1045 for details.

Allcall Addresses: An "allcall" is a general broadcast that does not request responses and does not designate any specific address. This can be in a global "allcall" or partial global "selective allcall" manner while not requesting responses. This essential function is required for emergencies ("HELP"), sounding data exchanges, and propagation and connectivity tracking.

Anycall Addresses: An ALE station may call and may receive responses from essentially unspecified stations, and it thereby can identify new stations and new connectivities. An "anycall" is a general broadcast which requests responses without designating any specific address(es). It is required for emergencies, reconstitution of network and systems, and creation of new networks. The anycall, selective-anycall, and double-selective anycall are characterized in Table X of FED-STD-1045A.

Net Addresses: The purpose of a net call is to establish contact rapidly and efficiently with multiple prearranged (net) stations (simultaneously, if possible) by the use of a single net address, which is an additional address assigned in common to all net members.

Group Address: The purpose of a group call is to establish contact with multiple non-prearranged (group) stations (simultaneously if possible) rapidly and efficiently by the use of a compact combination of their own addresses which are assigned individually.

Null Address: For test, maintenance, buffer times, and other purposes, the station can use a null address which is not directed to, accepted by, or responded to by any station. When an ALE station requires a null-address type of function, it can use the null address protocol. The null address special address pattern shall be "TO @@@," (or REPEAT @@@), if directly after another TO). The null address shall always use the TO (or REPEAT) and only in the calling cycle (T_{cc}). Null addresses may be mixed with other addresses (group call), in which case they shall appear only in the leading call (T_{1c}), and not in the scanning call (T_{sc}). Nulls will never be used in the conclusion (terminator) (THIS IS or THIS WAS). If a null address appears in a group call, no station is designated to respond in the associated slot; therefore, it remains empty (and may be used as a buffer for tuneups, or for overflow from the previous slot's responder, etc.).

Refer to FED-STD-1045 for additional information on station and network addresses.

Network manager addressing duties example

As an example of the duties of the network manager in a very large network one can look at the responsibilities of the HF ALE Network Manager in the HF Global Communications System Air/Ground/Air Network (see section 9.4 of this report). *The HF ALE Network Manager shall build and maintain a database of all their HF ALE stations, their configurations, ALE addresses, frequency lists, and system parameters. The manager must build databases and disseminate this information to all agencies supporting mission operation. The manager must work closely with frequency managers and their agency's tasking offices in order to build HF ALE networks* [HFALECoO, 1996].

HF ALE users of the HF Global Communications System Network must utilize addressing protocol procedures identified in the concept of operations (CONOPS) document to communicate with stations in this net. The goals of this document are to

-*Develop procedures that will ensure interoperability between DoD HF ALE users.*

1. Provide policy and procedures needed to establish a training and testing environment for HF ALE users,
2. Establish operational procedures that will ensure interoperability with other Federal agencies and connectivity to and from the National Command Authority (NCA).
3. Develop experience and generate *an operational data base for introducing HF ALE radio operations in the DoD.*[HFALECoO, 1996]

Network standard operating procedures

Every network has a set of standard operating procedures associated with its operation. These procedures establish protocol and permissive operation for purposes of establishing a network that is functional for all participants. Examples of standard operating procedures are:

1. Scan list: Setting up a scan list of individual radio parameters such as individual, net and group addresses. Every station may be assigned one or more individual (self-) addresses, and one or more net member (self-) addresses. Self-addresses—either individual or net—are identifiers that a station recognizes when receiving calls.

2. Sounding: Setting up to allow or disallow sounding—automatic or not—sounding interval, sound duration, sounding-retry time, etc., are operational parameters established in each individual node/radio. Sounding is the ability to empirically test selected channels (and propagation path) by providing a very brief, beacon-like, identifying broadcast which may be utilized by other stations to evaluate connectivity, propagation, and availability; and to select known channels for possible later use for communications. The sounding signal is a unilateral, one-way transmission which is performed at periodic intervals on unoccupied channels [FED-STD-1045]. Sounding may be used or not depending on the desires of the network manager and node personnel. If it is used, the following items need to be standard network operating

procedures administrated by the network manager: a) frequency of use, b) the amount of time it can be used, and c) the amount of time to wait after a faulty attempt.

3. Configuration parameters: Setting up individual radio parameters that will control calls; LQA updates, thresholds, maximum age, and reporting; network tune time; linking termination parameters; allow or disallow Anycalls or Allcalls; *etc.*

4. Message specific parameters: Setting up parameters considered specific to the individual message such as allowing or disallowing priority messages immediate message override *vs.* next break, *etc.*

5. Operational issues: Establishing operational procedures that will affect an individual station's communication within a network such as return to scan time, voice monitor, slot wait time, maximum slot used, net wait time, maximum wait before ACK, scan minimum dwell, *etc.*

6.2.3 Network Site Preparation

The third phase of network planning includes site preparation. Site preparation can include such things as contracts, permits, construction, and inspection. Few, if any of these items are typically the responsibility of the network manger unless some equipment is being installed that may not be the responsibility of the users, such as a master node unit or master control station which is common to all. The network manager will be responsible for site preparation details on common network equipment and will be an advisor regarding node equipment.

6.2.4 Network Installation

The fourth phase of network planning and implementation is the actual installation of equipment and procedures. The network manager must be involved in the installation of any common network equipment not the responsibility of the individual node stations. He also should be aware of the individual user□s installations and should offer assistance wherever possible.

6.2.5 Network Pre-Cutover

The fifth phase of network planning and implementation is the pre-cutover phase, which consists of the last-minute items necessary prior to operation. Prior to putting the network in operation, the following items should be completed: installation inspection, final tests, establishment of support systems, assurance of operator training, assurance of address and frequency coordination/installation, and a check of network documentation.

Assist users in network setup and operation

The network manager is the person to consult when first beginning to set up a network or when a question arises over station operation. The network manager might be involved from the beginning with procurement issues, he will assign addresses and frequencies, he will establish operator training guidelines, and will be responsible for user training.

Frequency coordination/installation

The radios typically require the installation of address parameters as well as frequencies and frequency sets. The network manager can be involved to whatever extent necessary to assure that all users are ready for a smooth cutover.

6.2.6 Network Cutover

The sixth phase of network planning and implementation is the actual cutover phase where actual network operation begins. The network manager needs to schedule and to coordinate the cutover operation. He should assure that coverage is as anticipated in the design plan during the cutover period. He should try to determine that traffic patterns are as expected between the various nodes. He must also be prepared with a contingency plan, should things not occur as planned.

6.2.7 Network Operations

The seventh and final phase is the operation of the network. Once a system has been successfully installed, tested, and placed into operation, then the day-to-day management of the network begins. Operations deals with monitoring, control, diagnostics, and repair. The network manger should be instrumental in assuring that the network operates smoothly and efficiently. He should be responsible for continued configuration management, resolving network problems or faults, monitoring network performance/operations, network maintenance, user satisfaction, frequency and address maintenance, and network security.

Maintaining operational control may mean establishing a control center, complete with procedures for reporting problems, facilities for monitoring, and tools for support.

Continued configuration management

As an on-going task, the network manager must monitor the routes that information takes through the network and must compare it to the original details established during planning. Changes may be necessary in frequencies, frequency groups, addresses, nets, antennas, power, *etc.*, to correct an undesirable situation.

Resolve network problems or faults

The network manager must be notified when any network node or element has failed, is likely to be near failure, or is performing outside of its range of defined specifications. The network manager has the task of monitoring network conditions to detect out-of-tolerance behavior and then taking action when such conditions occur. A network cannot be found that will not have an occasional problem or glitch in its operation. Interference issues, grouping issues, operator errors due to poor training, etc., are a few of the issues that a network manager must deal with on a day-to-day basis. He must be prepared with knowledge concerning the network, standard operating procedures, assignments, and training issues, so that he/she is able to resolve misunderstanding or technical issues.

Performance management

The network manager is responsible for supervising the performance of the network and for controlling the flow of traffic to obtain maximum use of the network capacity. This task includes monitoring the network's traffic, its remaining capacity, the rate of flow, the incidents of delay, and other factors relating to the network's connection and flow services. This task also includes capacity management and planning functions. A summary of the specific work functions of the network manager might include:

- Monitoring the flow of traffic in the network on a real-time basis;
- Collecting and analyzing network performance data;
- Identifying abnormal network situations; and
- Investigating and determining the reasons for network traffic-flow problems.

Network maintenance

To support the network after implementation, maintenance procedures must be developed to maintain the hardware and software. These procedures can include preventative maintenance steps designed to protect both the hardware and software associated with the network. On the hardware side, procedures should be established to protect network equipment from premature failure. On the software side, procedures should be established to continually monitor the system responsiveness and traffic throughput. Also checks should be made to see if the latest version of software is being used. Checks should be made on buffers and matrixes to see that they are not becoming full or filled with useless information. Problem resolution can be at the network level or at the individual node level, but in all cases a report to the network manager should be required if the problem affects some aspect of the network. The network manager should be made aware of immediate and potential problems so that a pattern of trends might be established. He/she needs to be given enough information so that he/she is able to make changes in equipment, software, or procedures. The network manager will be key to tracking problem resolution and dispatching technicians/ programmers to solve problems.

Once procedures are in place, user training of personnel on maintenance concepts should be undertaken.

User satisfaction

User satisfaction implies the network must receive high marks in the areas of performance, availability, and reliability. User satisfaction can also be enhanced by supplying users with the latest information on system changes and by providing users with formal and informal training. The users of the network are the individuals and organizations with a mission, the network is their communication tool to bring about that mission. Keeping the users happy while at the same time operating an efficiently functioning network is a key task for the network manager.

Items that are keys to good user satisfaction include:

Good performance: Good performance means a predictable response time to message requests. In the HF ALE Radio system, the network manager has little control over the message processing and node operating parameters. He does, however, have control over the configuration aspects of the network. The configuration details include the number of users, user s message types, and hardware employed; all can affect the network performance.

Availability: Availability means that all necessary components are operable when the user requires them. For HF ALE radio systems this means availability or access to the radio media on demand or within a reasonable time period. But since HF propagation on one particular channel is not available at all times, availability will be construed to mean over at least one HF propagation path.

Reliability: Reliability of the network involves error characteristics of the medium and stability of the hardware and software components. Again, the network manager has little control over the varying conditions of the HF propagation paths but the stability of the hardware and software comes from good planning, good procurement, and good maintenance practices. These are issues that can be addressed by the network manager.

Repairing failures in a network: When failures occur, the network manager and his team must either patch around the failure, replace the failed component, or repair it.

Keeping Users Informed: In addition to performance, availability, and reliability, there are a number of other factors, less obvious, that can affect user satisfaction. Users should be informed of scheduled down time, periods of bad propagation conditions, certain changes in hardware and software, and changes in personnel with whom those users will be interfacing.

Frequency and address maintenance

As an on-going task, the network manager will review the frequency and frequency set assignments to determine if the choices are still the most efficient possible. The address choices should also be reviewed to determine if any details have changed and if the address scheme is still the most efficient possible.

Security management

The network manager has the task of controlling access to the network. In the case of a network such as an HF ALE radio system, access control will probably be by controlling the frequency and address components of the system to prevent illegal entry. The network manager must be aware of the possibility that security issues might arise at any time, and he/she must be prepared to resolve them. The network manager should have in place a procedure for resolving security issues. The following items could be used as examples for establishing a process for managing security risks:

1. Identify vulnerabilities of the network,
2. Analyze the likelihood of threats to the network,
3. Assess the consequences if each threat were carried out,
4. Estimate cost of each attack, and
5. Identify and cost out the potential countermeasures.
6. Select the security mechanisms that are justified. [Minoli, 1991]

Vulnerabilities to the network and the means of counteracting might be described as follows:

1. Physical security vulnerabilities. Protection for the physical aspects of the system such as equipment and facilities from such things as fires, floods, thief, abuse, etc. Usually common sense measures are what is required for protection against physical vulnerabilities (*i.e.* fire equipment, power protection systems, secured building, restricting physical access, *etc.)*

2. Personnel vulnerabilities. One of the principle threats to sensitive information or equipment has always been the individuals who are trusted to properly handle this responsibility [Walker, 1985]. The network manager must assure that principals associated with the network and network information are the only individuals exposed to sensitive information.

3. Procedural vulnerabilities. It is necessary to have a reasonable and complete set of procedures for the operation of the network. User passwords, system use procedures, outage recovery procedures, etc are all important to a smooth functioning network operation.

The vulnerability of the network constitutes a wide range of vulnerabilities in which failure of any element may compromise the integrity of the entire system [Walker *et al.,* 1985]

Security threats to a network might include:

1. Circumventing the access procedures and entering the network illegally;
2. Denial of service by jamming (through a tone or signal), or suppressing traffic by generating nuisance traffic;
3. A masquerade attack in which an entity claims to be a different entity;
4. Modification of messages by spurious signals or *etc.;*
5. A replay attack that is carried out when a message, or part of a message, is repeated in order to produce an unauthorized effect;
6. A trapdoor implanted when an entity of the system is modified to allow an attacker to produce a future unauthorized effect on a command or an predetermined event; and
7 A Trojan horse is an entity that, when innocuously introduced into the system, has deliberately planned unauthorized effect in addition to its authorized function.[Minoli, 1991].

If security mechanisms or countermeasures are deemed appropriate for the network, the following guidelines will aid the network manager in their use. Security controls and mechanisms are effective if they make the cost of obtaining or modifying data, and/or disrupting services greater than the potential value of carrying out the disruption. Security measures will usually increase the cost of the systems; therefore, the specific threats, if any, should be identified. Some controls that could be used in a HF ALE system might include:
- configuration of the system as a star, with strict controls imposed for host access;
- encryption and use of keys;
- node and hub, physical access controls;
- frequency and address management;
- call back; and
- message authentication. [Minoli, 1991]

The duties of the network manager in regards to security might include:

1. The creation, deletion, and control of security services and mechanisms;
2. The distribution of security-relevant information; and
3. The reporting of security-relevant events.

6.3 Automated HF Network Management

HF ALE radios are presently using automation to the extent of assisting the operator with establishment of the link, and passing traffic over marginal HF channels (those channels experiencing fading, or noise interference). Additional features and functions are being considered that would extend the requirements of the automated network management system and thus increasing the duties of the network manager. These features and functions might include:

1. monitoring and reporting network status (connectivity, capabilities, congestion, faults, *etc*.);
2. updating network routing tables;
3. manipulating the operating data of automated communications controllers (such as ALE controllers);
4. identifying software versions and updating the software, in ALE and other communication controllers;
5. rekeying linking-protection scramblers; and
6. remotely operating all communications equipment, which includes adjusting transmitter power of linked stations, reading meters, and rotating antennas.[Johnson *et al.,* 1997]

Annex 4 of this document contains some examples of typical HF ALE radio networks.

6.4 Conclusion

The network planning and design process is not difficult when one understands just what is to be accomplished. One simply remembers the fundamental steps for network planning: define the *network's scope*, collected together the *objectives and requirements*, do a *benefits and cost analysis*, and complete a *network design plan* to start the ball rolling. An *implementation plan, site plan, installation plan and cutover plan* gets your network running. While a good *operations plan* will keep the network running efficiently.

As the role for communication networks expands, so will the role and importance of network management. The keys to effective network management are personnel who are competent and knowledgeable, and who can plan a network for a wide range of uses, and who can work well with wide spectrum of users. With careful management, the network can be a valuable asset to the communication users of typical HF ALE radio systems.